ABSTRACT OF THE DISCLOSURE

Bits of a first bit sequence are rearranged in a first matrix according to a predetermined arrangement rule. The first bit sequence represents information being a base of a key. Blocks are formed in the first matrix. Each of the blocks has bits, the number of which is smaller than the number of bits composing the first matrix. Logical operation is executed among bits in each of the blocks, and a bit being a result of the logical operation is generated. The logical-operation-result bits are combined into a second bit sequence. The number of bits composing the second bit sequence is smaller than the number of bits composing the first bit sequence. There is a second matrix composed of predetermined third bit sequences. The second matrix is accessed and one is read out from among the third bit sequences in response to the second bit sequence. The read-out third bit sequence is outputted as information representative of the key. The number of bits composing each of the third bit sequences is smaller than the number of bits composing the second bit sequence.

0021257960